EJERCICIOS SHODAN

Prerrequisitos

Registrarse en:

https://www.shodan.io/

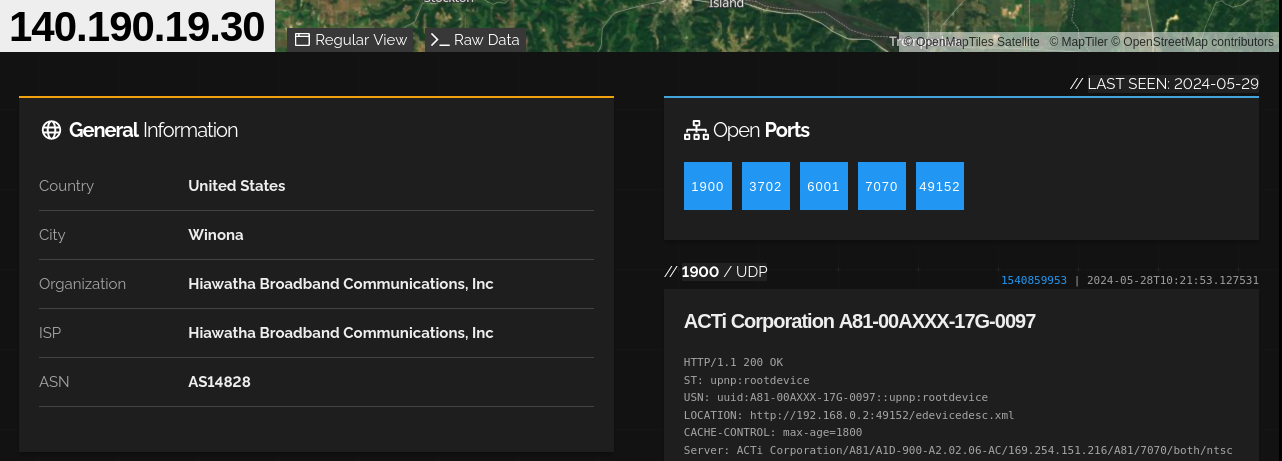
Utilizar filtros para acotar las siguientes búsquedas y responder las preguntas.

Ejercicio 1

Busca una webcam e intenta acceder a ella usando el nombre de usuario y la contraseña por defecto. Entrega una captura de pantalla donde se vea la localización de la cámara, el país, el proveedor de internet, los puertos abiertos…

Lista de contraseñas y/o nombre de usuario predeterminado de IP´s de cámaras:

https://netviewcctv.co.uk/blog/ipcampassword/



Ejercicio 2

Intenta acceder a un router con el nombre de usuario y la contraseña por defecto. No hagas ninguna modificación. Razona tu respuesta: ¿crees que es legal hacer una modificación a la configuración de un router al que puedas acceder?

En general, acceder a un router con credenciales por defecto sin autorización puede ser considerado como una violación de la privacidad y la seguridad, y en muchos casos puede ser ilegal y constituir un delito de acceso no autorizado a un sistema informático. Sin embargo, en algunos casos, como en entornos de pruebas autorizadas o en situaciones donde se tiene permiso explícito del propietario del router para realizar cambios en su configuración, podría ser legal y ético modificar la configuración del router.

Ejercicio 3

Comprueba si hay algún sistema con “Windows XP” conectado a internet, ¿en qué país?, ¿qué puerto está exponiendo?. Razona tu respuesta: ¿qué problemas de seguridad puede tener?, ¿por qué?

No he encontrado ninguno y aunque es posible encontrar sistemas Windows XP conectados a Internet, estos representan un riesgo significativo para la seguridad debido a su falta de soporte y las vulnerabilidades conocidas que no se han parcheado. Es importante que los propietarios de estos sistemas tomen medidas para mitigar estos riesgos, como actualizar a sistemas operativos más recientes y aplicar medidas de seguridad adicionales.

Ejercicio 4

El siguiente enlace nos muestra el estado de la seguridad informática de España, según Shodan:

https://exposure.shodan.io/#/ES

Interpretando el mapa indica la siguiente información:

¿Cuántos puertos abiertos hay en España?, ¿cuál es el más usado?, ¿a qué servicio corresponde?

5,832,639 - 161 - SNMP

¿Cuántos sistemas de control industriales están conectados a internet?

8,118

¿Cuántas páginas web utilizan el protocolo obsoleto SSLv2 en el protocolo https?

No está disponible la información

¿Qué porcentaje de servidores SAMBA no tienen habilitados un sistema de autentificación?

9.6%

¿Cuántas bases de datos están comprometidas?

100

¿Cuál es la vulnerabilidad más detectada? A qué fallo corresponde.

CVE-2015-0204 - Debilidad en las claves RSA

Ejercicio 5

La ciberseguridad industrial es cada vez más importante. ¿Cómo buscarías PLCs de Siemens del modelo S7 que estén conectados a Internet usando Google y usando Shodan?

intitle:"Siemens Simatic S7" inurl:"/portal/" - "Siemens" "S7" "CPU"

Una vez que los hubieras encontrado, ¿cuál es el usuario y contraseña por defecto de este tipo de dispositivos? NOTA: Sólo puedes realizar las búsquedas, no entres en ninguno de los paneles que encuentres.

admin - admin

Ejercicio 6

¿Cómo podrías saber qué software se ha utilizado para montar un servidor web determinado (Apache, IIS, etc.)? ¿Y su versión específica? curl -I - nikto -h

Ejercicio 7

¿Cómo podrías localizar los puertos en los que un servidor emplea SSL ó TLS? ¿Y cómo podrías saber si el cifrado que se está usando es débil?

nmap -sV --script ssl-enum-ciphers -p 443,465,993,995